CLMPTO
02/13/2002
Y.V.

1. A storage device including a trusted clock, a memory, a time-stamper and a digital signer, the device being adapted in use to store to said memory data that has been time-stamped by said time-stamper, with a time obtained from said trusted clock, and digitally signed with a digital signature by said digital signer.

2. A device as claimed in claim 1 wherein said memory comprises either of the following: a disc, a tape drive.

3. A device as claimed in claim 1 wherein said memory is a long term storage medium.

4. A device as claimed in claim 1 wherein said memory is removable from the storage device.

5. A device as claimed in claim 1 wherein said device comprises a part of any one of the following: a disc drive, a tape drive, a disc array, a disc sub-system, a tape library, an optical jukebox, a disaggregated storage network, a storage area network, network attached storage.

6. A device as claimed in claim 1 wherein said trusted clock is provided by a card adapted to be plugged into said device.

7. A device as claimed in claim 1 wherein said trusted clock is an encapsulated hardwired component.

8. A device as claimed in claim 1 wherein there is a controller, with associated controller logic, said controller logic being protected by a trusted mechanism to prevent unauthorised and unnoticed alteration of said controller logic.

9. A device as claimed in claim 1 wherein said device has a controller adapted to do at least one of the following: identify whether data received by said device has a flag indicative as a command to time-stamp flagged data, identify whether command language used to control operation of said device has a marker indicative as a command to time-stamp selected data, check whether the time-stamper is set to a time-stamp mode to time-stamp received data, or not, so set so as not to time-stamp data.

10. A device as claimed in claim 1 further comprising a clock-correcting input adapted to input a trusted correction signal to said trusted clock to correct said clock.

11. A device as claimed in claim 1 which has no significant functional capability beyond that claimed in claim 1 and which is incapable of general computational activities.

12. A storage device including a trusted clock; a long term memory device; a time-stamper; a digital signing unit; and a controller, with associated controller logic: said device being adapted, in use, to store to said memory device data that has been time-stamped by said time-stamper with a time obtained from said trusted clock and digitally signed with a digital signature by said digital signing unit, and said controller logic being protected by a trusted mechanism to prevent, in use, unauthorised alteration of said controller logic.

13. A storage device including trusted clock means for non-repudiably measuring time, data storage means for storing data, time-stamping means for stamping data with a non-repudiable time supplied by said trusted clock means, digital signing means for signing data digitally such that said data storage means stores data that has been time-stamped by said time-

stamping means and signed with a digital signature by said digital signing means, in use.

14. (Amended) A method of storing secure time-stamped data in a data storage device, a trusted clock being at the data storage device, comprising the steps of:

(i) timestamping data by using the trusted clock at said data storage device;

(ii) creating a digital signature dependent upon content of said data and time-stamp; and

(iii) storing said data and the signature associated with said data in said data storage device on a recording medium of said data storage device.

15. (Amended) A method as claimed in claim 14 where said data storage device comprises a long-term data storage medium and wherein time-stamped, signed data are stored on said long-term data storage medium.

16. (Amended) A method as claimed in claim 14 wherein a controller is used to control operations (i) to (iii), and wherein said controller is controlled by control logic, and protecting said control logic by a trusted mechanism which ensures that said control logic has not been modified from what it should be.

17. (Amended) A method as claimed in claim 14 further including checking data received by said data storage device for a flag indicative of instructions to time-stamp all of or a selected part of said data, and said data, or the part of said data, is time stamped accordingly.

18. (Amended) A method as claimed in claim 14 further including checking a command language of a controller for instructions to time-stamp all, or a selected part, or parts, of said data.

19. A method as claimed in claim 14 wherein said device is controlled by a controller which has a time-stamp setting in which the time-stamper time-stamps said data and a non time-stamping setting in which the time-stamper does not time-stamp said data, and in which a check is made as to the setting of said controller prior to said time-stamping, or not, of received said data.

20. A method as claimed in claim 14 comprising transmitting said data to said device over the Internet or other public network, and time-stamping and signing said data, and storing said time-stamped signed data, within said data storage device without transmitting said signed data back over the Internet or other public network.

21. A method as claimed in claim 14 wherein said data that is time-stamped is a digest of a larger data record.

22. (Amended) A method of storing time-stamped data in an arrangement including (a) a data storage device having a long term data storage medium, (b) a trusted clock at said data storage

device; and (c) a controller at said storage device, the controller being associated with control logic that is protected by a trusted mechanism, the method comprising the steps of:

(i) using the trusted clock to time stamp said data at said data storage device, under the control of said controller;

(ii) creating a digital signature dependent upon content of said data and time-stamp, under the control of said controller; and

(iii) storing said data and associated signature on said long term data storage medium of the data storage device, under the control of said controller.

23. A network having a data storage device adapted to time-stamp and store data that it receives from said network without transmitting time-stamped data across said network.

24. (Amended) Software, firmware or a computer readable medium having a program recorded thereupon which, in use, causes a processor of a data storage device running a program to execute a process including:

i) time-stamping data at said data storage device;

ii) creating a digital signature dependent upon content of said data and time-stamp; and

iii) storing said data and associated said signature on a recording medium of said data storage device.

25. Software, firmware or a computer readable medium having a program recorded thereupon which when operable upon a control processor of a data storage device causes the device to operate as a device including a trusted clock, a memory, a time-stamper and a digital signer, the device being adapted, in use, to store to said memory data that has been time-stamped by said time-stamper, with a time obtained from said trusted clock and digitally signed with a digital signature by said digital signer.

26. (Amended) A method of storing time-stamper data on a network comprising transmitting the data from a first, remote, network-attached device to a data storage device, the data storage device including a trusted clock, a memory, a time-stamper and a digital signer, storing in said memory data that have been time-stamped by said time-stamper, the stored data including a time obtained from said trusted clock and digitally signed with a digital signature by said digital signer, in the absence of transmitting time-stamped data back to said remote device for storage.